

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-215172

(P2000-215172A)

(43) 公開日 平成12年8月4日(2000.8.4)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 F 5 B 0 4 3
			3 3 0 G 5 B 0 8 5
G 0 6 T 7/00		15/62	4 6 0 5 J 1 0 4
H 0 4 L 9/32			4 6 5 K
		H 0 4 L 9/00	6 7 3 D
審査請求 有 請求項の数 7 O L (全 7 頁) 最終頁に続く			

(21) 出願番号 特願平11-12452

(22) 出願日 平成11年1月20日(1999.1.20)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 住野 徹

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100108578

弁理士 高橋 詔男 (外3名)

Fターム(参考) 5B043 AA09 BA01 BA02 CA10 FA04  
GA18

5B085 AE03 AE12 AE26

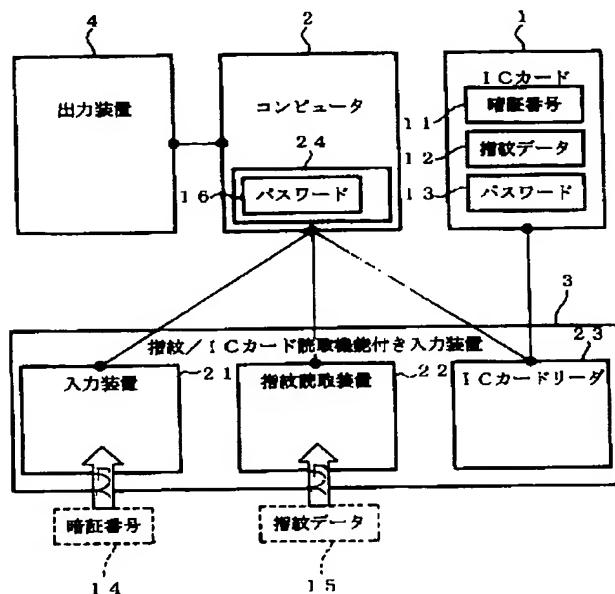
5J104 AA07 KA01 KA17 NA05 NA35

(54) 【発明の名称】 個人認証システム

(57) 【要約】

【課題】 個人認証を必要とする業務における情報機器の使用管理をより堅牢なセキュリティで実現することができる個人認証システムを提供する。

【解決手段】 情報機器2の使用者を認証するシステムであって、登録された使用者であることを特定できる生体情報12及びパスワード13が格納された個人認証用のカード1と、カード1に格納された生体情報12及びパスワード13を読み取るカード読取装置23と、使用者から生体情報15を読み取る生体情報読取装置22と、カード読取装置23から出力される生体情報12及びパスワード13と、生体情報読取装置22から出力される生体情報15及び情報機器2に格納されているパスワード16とを照合する照合装置24とを備えたことを特徴とする。



## 【特許請求の範囲】

【請求項 1】 情報機器の利用者を認証するシステムであって、

登録された利用者であることを特定できる生体情報及びパスワードが格納された個人認証用のカードと、該カードに格納された前記生体情報及びパスワードを読み取るカード読取装置と、利用者から生体情報を読み取る生体情報読取装置と、前記カード読取装置から出力される生体情報及びパスワードと、前記生体情報読取装置から出力される生体情報及び前記情報機器に格納されているパスワードとを照合する照合装置とを備えたことを特徴とする個人認証システム。

【請求項 2】 前記情報機器には、利用者が識別番号を入力する識別番号入力装置が設けられ、前記カードには、登録された利用者であることを特定できる識別番号が格納されるとともに、格納された該識別番号と、前記識別番号入力装置より入力された識別番号とを照合する照合手段を備えたことを特徴とする請求項 1 記載の個人認証システム。

【請求項 3】 前記生体情報は、指紋データであることを特徴とする請求項 1 または 2 記載の個人認証システム。

【請求項 4】 前記指紋データは、複数の指紋データであることを特徴とする請求項 3 記載の個人認証システム。

【請求項 5】 前記カードは、少なくとも登録された利用者であることを特定できる生体情報及びパスワードが電気信号として記憶された IC カードであることを特徴とする請求項 1 ないし 4 のいずれか 1 項記載の個人認証システム。

【請求項 6】 前記生体情報、パスワードまたは識別番号、のいずれか 1 つまたは 2 つ以上をアルゴリズムにより暗号化したことを特徴とする請求項 1 ないし 5 のいずれか 1 項記載の個人認証システム。

【請求項 7】 前記カード読取装置と、前記識別番号入力装置と、前記生体情報読取装置とを一体化したことを特徴とする請求 2 ないし 6 のいずれか 1 項記載の個人認証システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、個人認証システムに関し、特に、情報機器起動時に利用者を認証する際に用いて好適な個人認証システムに関するものである。

## 【0002】

【従来の技術】 近年、コンピュータの普及が進むにつれて、データの盗難や改ざん、あるいは第三者が正当な使用者に成りすます等、コンピュータの不正利用を利用した問題が増加してきている。この問題に対し、従来より行われている対策としては、主に暗証番号のようなパスワード入力を要求するものが一般的であったが、このパ

スワードはあくまでも個人の知識であるために、漏洩したり他人に盗まれたりして不正使用される等の問題があった。

【0003】 そこで、最近では、個人情報等を格納した IC カードを利用した個人認証も数多く提案され、一部では実用化されてきている。この IC カードでは、通常、該 IC カードの内容をアクセスするためにはパスワード入力が必要とされているケースが多いため、上述したパスワードのみの個人認証よりは安全性が高くなっている。

## 【0004】

【発明が解決しようとする課題】 ところで、従来の IC カードを利用した個人認証では、物理的な IC カードと個人の知識であるパスワードを盗まれてしまうと、やはり安全性が破られてしまうという問題点があった。一方、指紋など個人の生体情報は個人毎に異なるため、個人を特定するための手段として最近注目されている。しかしながら、この生体情報を認証に用いる方法では、怪我などで生体情報が変わってしまった、あるいは装置の性能によって誤認識される場合があるという問題点もある。

【0005】 本発明は、上記の事情に鑑みてなされたものであって、個人認証を必要とする業務における情報機器の使用管理をより堅牢なセキュリティで実現することができる個人認証システムを提供することを目的とする。

## 【0006】

【課題を解決するための手段】 上記課題を解決するために、本発明は次の様な個人認証システムを提供した。すなわち、請求項 1 記載の個人認証システムは、情報機器の利用者を認証するシステムであって、登録された利用者であることを特定できる生体情報及びパスワードが格納された個人認証用のカードと、該カードに格納された前記生体情報及びパスワードを読み取るカード読取装置と、利用者から生体情報を読み取る生体情報読取装置と、前記カード読取装置から出力される生体情報及びパスワードと、前記生体情報読取装置から出力される生体情報及び前記情報機器に格納されているパスワードとを照合する照合装置とを備えたことを特徴としている。

【0007】 請求項 2 記載の個人認証システムは、請求項 1 記載の個人認証システムにおいて、前記情報機器には、利用者が識別番号を入力する識別番号入力装置が設けられ、前記カードには、登録された利用者であることを特定できる識別番号が格納されるとともに、格納された該識別番号と、前記識別番号入力装置より入力された識別番号とを照合する照合手段を備えたことを特徴としている。

【0008】 請求項 3 記載の個人認証システムは、請求項 1 または 2 記載の個人認証システムにおいて、前記生体情報は、指紋データであることを特徴としている。

【0009】請求項4記載の個人認証システムは、請求項3記載の個人認証システムにおいて、前記指紋データは、複数の指紋データであることを特徴としている。

【0010】請求項5記載の個人認証システムは、請求項1ないし4のいずれか1項記載の個人認証システムにおいて、前記カードは、少なくとも登録された使用者であることを特定できる生体情報及びパスワードが電気信号として記憶されたICカードであることを特徴としている。

【0011】請求項6記載の個人認証システムは、請求項1ないし5のいずれか1項記載の個人認証システムにおいて、前記生体情報、パスワードまたは識別番号、のいずれか1つまたは2つ以上をアルゴリズムにより暗号化したことを特徴としている。

【0012】請求項7記載の個人認証システムは、請求項2ないし6のいずれか1項記載の個人認証システムにおいて、前記カード読取装置と、前記識別番号入力装置と、前記生体情報読取装置とを一体化したことを特徴としている。

#### 【0013】

【発明の実施の形態】本発明の個人認証システムの一実施形態について図面にに基づき説明する。図1は本発明の一実施形態の個人認証システムが適用されたコンピュータ・システムを示す概略構成図であり、登録された使用者であることを特定できる個人情報を格納するICカード1と、使用者個人の認証を必要としプログラム制御により動作するコンピュータ（情報機器）2と、指紋／ICカード読取機能付き入力装置（以下、各種機能付入力装置と称する）3と、表示機能を有しコンピュータ2のプログラム処理結果を出力または表示する出力装置4とにより構成されている。

【0014】ICカード1には、暗証番号（識別番号）11、指紋データ（生体情報）12、コンピュータ2起動用のパスワード13等の各種情報が格納されている。各種機能付入力装置3は、暗証番号14を入力する入力装置（識別番号入力装置）21と、指紋データ（生体情報）15を図形データとして入力する指紋読取装置（生体情報読取装置）22と、ICカード1から暗証番号11、指紋データ12、パスワード13等を読み取るICカードリーダ（カード読取装置）23とを備えている。

【0015】コンピュータ2には、使用者であることを特定できるパスワード16が登録され、かつ、ICカードリーダ23から出力される指紋データ12、パスワード13等のデータと、指紋読取装置22から出力される指紋データ15及び該コンピュータ2に登録されているパスワード16を照合する照合装置24が内蔵されている。この照合装置24により照合された結果は、出力装置4により出力または表示される。なお、前記ICカード1には、暗証番号11により指紋データ12とパスワード13へのアクセスを制御する保護手段、及び暗証番

号入力装置21より入力された暗証番号14と該ICカード1に格納された暗証番号11とを照合する照合手段が備えられている。

【0016】次に、このコンピュータ・システムの動作について、図1及び図2に基づき説明する。まず、コンピュータの使用者は、コンピュータ2の電源を投入し（ステップA1）、ICカード1をICカードリーダ23に挿入する（ステップA2）。次に、ICカード1が正常に挿入されているか否かの確認が実施され（ステップA3）、正常に挿入されていない場合には、ICカード1の挿入を要求するメッセージが出力装置4に表示される（ステップA4）。一方、ICカード1が正常に挿入されている場合には、次のステップに進む。

【0017】次に、ICカード1に格納されている指紋データ12やパスワード13等をアクセスするのに必要となる暗証番号14の入力要求メッセージが出力装置4に表示される（ステップA5）。使用者は暗証番号入力装置21により暗証番号14を入力する（ステップA6）。コンピュータ2はこの暗証番号14をICカードリーダ23に送り、ICカード1によって該暗証番号14と格納されている暗証番号11との照合が実施される（ステップA7）。

【0018】暗証番号11、14が互いに一致しない場合は、ICカード1の正当な使用者でない旨のメッセージを出力装置4に表示し、コンピュータ2の起動処理を終了する（ステップA8）。また、暗証番号11、14が互いに一致した場合は、次のステップに進む。なお、ICカードリーダ23に格納されている指紋データ12とコンピュータ起動用パスワード13は暗証番号11によって保護されているため、上記照合が失敗した場合は、これ以降、内容を読み出すことは不可能である。

【0019】コンピュータ2は、更に、使用者に指紋読取装置22に指を置く旨のメッセージを出力装置4に表示し（ステップA9）、指紋データ15をコンピュータ2に読み取る（ステップA10）。次いで、コンピュータ2により上記指紋データ15とICカード1に格納されている指紋データ12を照合する（ステップA11）。ここで、指紋データ12、15が互いに一致しない場合には、ICカード1の正当な使用者でない旨のメッセージを出力装置4に表示してコンピュータ2の起動処理を終了する（ステップA8）。また、指紋データ12、15が互いに一致した場合は、次のステップに進む。

【0020】最後に、コンピュータ2は、内蔵する照合装置24により、コンピュータ起動用のパスワード13をICカード1より読み出し、コンピュータ2内に格納されているパスワード16との照合を実施する（ステップA12）。ここで、パスワード13、16が互いに一致しない場合には、そのコンピュータ2の正当な使用者でない旨のメッセージを出力装置4に表示し、コンピュ

ータ 2 の起動処理を終了する（ステップ A 1 3）。また、パスワード 1 3、1 6 が互いに一致した場合は、コンピュータ 2 の起動処理を続行する（ステップ A 1 4）。

【0021】本実施形態のコンピュータ・システムによれば、ICカード 1 に格納されている暗証番号 1 1、指紋データ 1 2 及びコンピュータ 2 起動用のパスワード 1 3 と、暗証番号入力装置 2 1 から入力される暗証番号 1 4、指紋読取装置 2 2 から入力される指紋データ 1 5 及びコンピュータ 2 に登録されているパスワード 1 6 とを照合するというように、複数レベルで個人認証を行なうことができるので、正当な使用者ではない者によるコンピュータの不正使用を防止することができる。

【0022】また、暗証番号入力装置 2 1、指紋読取装置 2 2 及び IC カードリーダ 2 3 を一つの各種機能付入力装置 3 に統合したので、コンピュータ 2 と各種機能付入力装置 3 との間の通信を一本にまとめることができ、盗聴によるデータの漏洩等をより堅牢に防ぐことができる。

【0023】以上、本発明の個人認証システムが適用されたコンピュータ・システムの一実施形態について図面に基づき説明してきたが、具体的な構成は本実施形態に限定されるものではなく、本発明の要旨を逸脱しない範囲で設計の変更等が可能である。例えば、本実施形態では、ICカード 1 に 1 つの指紋データ 1 2 を格納する構成としたが、ICカード 1 に、複数（種）の指紋データ 1 2 を格納する構成としてもよい。この場合、複数（種）の指紋データ 1 2 を格納しておくことで、怪我などで一部の指紋データ 1 2 が変化してしまった場合等においても、残った他の指紋データ 1 2 を用いて個人認証を実行することができるという優れた効果がある。

【0024】また、入力装置 2 1 より入力する暗証番号 1 4、指紋読取装置 2 2 より入力する指紋データ 1 5、コンピュータ 2 に格納されているコンピュータ起動用のパスワード 1 6、ICカード 1 に格納されている暗証番号 1 1、指紋データ 1 2 及びコンピュータ起動用のパスワード 1 3 等を、既知のアルゴリズムを利用して暗号化してもよい。この場合、各装置間を行き来する個人情報データを暗号化することにより、盗聴によるデータの漏洩等を

より堅牢に防ぐことができるという優れた効果がある。

#### 【0025】

【発明の効果】以上説明した様に、本発明によれば、登録された使用者であることを特定できる生体情報及びパスワードが格納された個人認証用のカードと、該カードに格納された前記生体情報及びパスワードを読み取るカード読取装置と、使用者から生体情報を読み取る生体情報読取装置と、前記カード読取装置から出力される生体情報及びパスワードと、前記生体情報読取装置から出力される生体情報及び前記情報機器に格納されているパスワードとを照合する照合装置とを備えたので、生体情報及びパスワードを照合することで、複数レベルで個人認証を行なうことができるので、正当な使用者ではない者によるコンピュータの不正使用を防止することができる。したがって、使用者個人の認証を必要とする業務における情報機器の使用管理をより堅牢なセキュリティで実現することができる。

#### 【図面の簡単な説明】

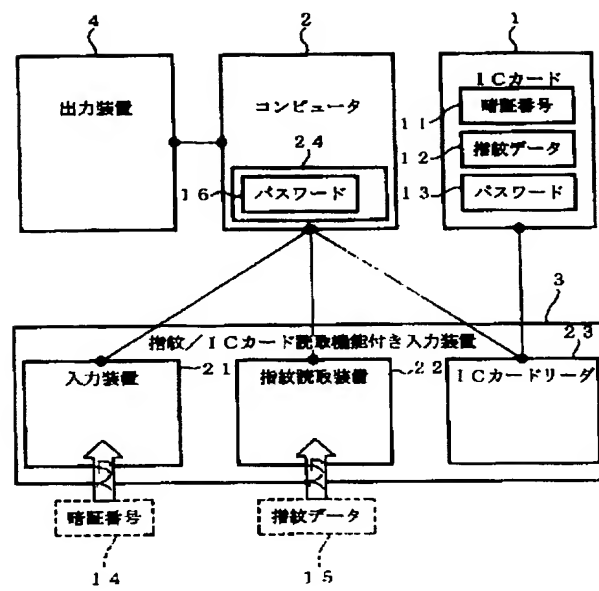
【図 1】 本発明の一実施形態の個人認証システムが適用されたコンピュータ・システムを示す概略構成図である。

【図 2】 本発明の一実施形態の個人認証システムが適用されたコンピュータ・システムの動作を示す流れ図である。

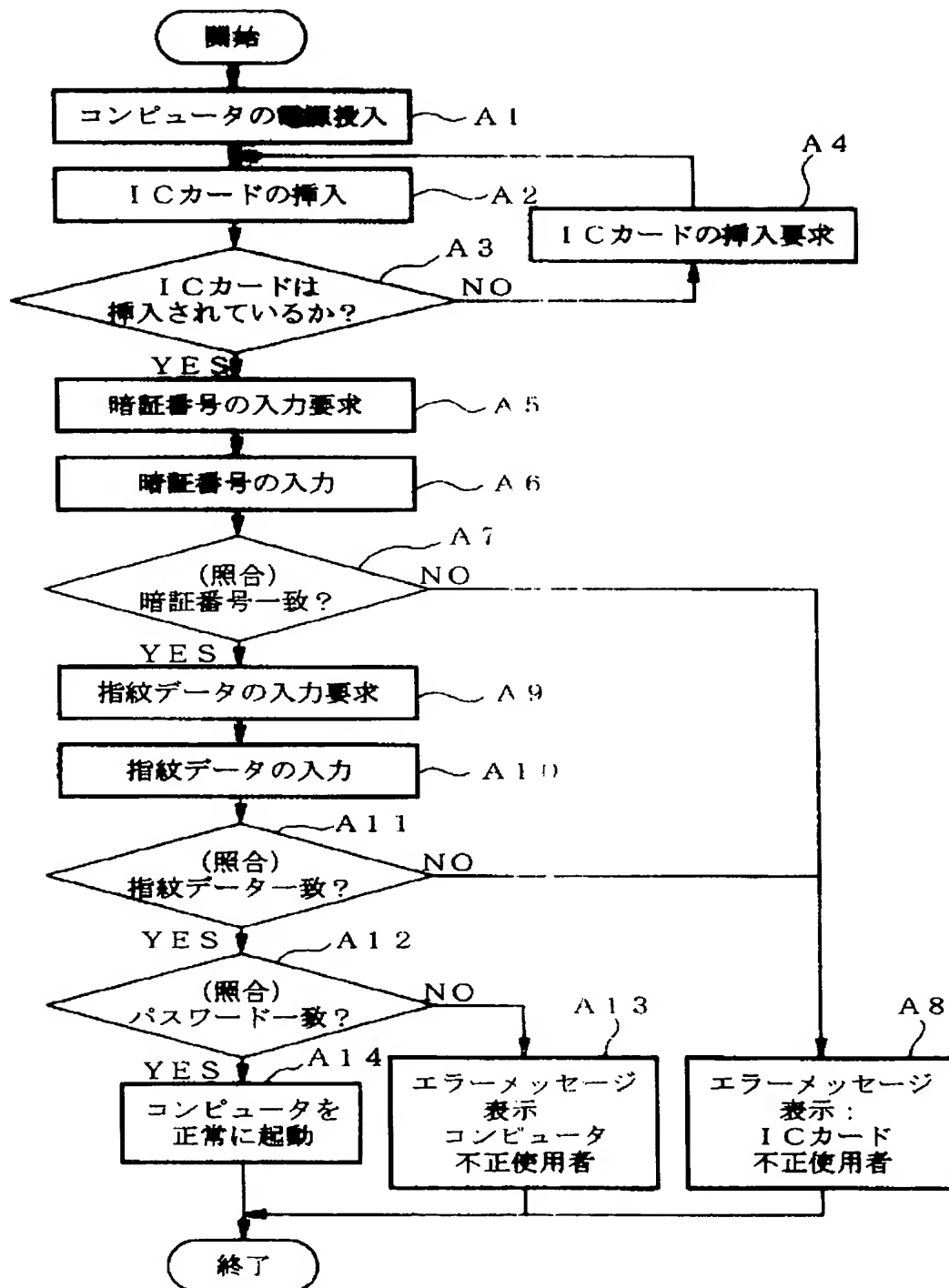
#### 【符号の説明】

- 1 IC カード
- 2 コンピュータ（情報機器）
- 3 指紋／IC カード読取機能付き入力装置
- 4 出力装置
- 11 暗証番号（識別番号）
- 12 指紋データ（生体情報）
- 13 パスワード
- 14 暗証番号
- 15 指紋データ（生体情報）
- 16 パスワード
- 21 入力装置（識別番号入力装置）
- 22 指紋読取装置（生体情報読取装置）
- 23 IC カードリーダ（カード読取装置）
- 24 照合装置

【図1】



【図 2】



BEST AVAILABLE COPY

フロントページの続き

(51) Int. Cl.<sup>7</sup>

識別記号

F I  
H O 4 L 9/00

テーマコード(参考)

6 7 3 E  
6 7 3 A